

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
3. April 2003 (03.04.2003)

PCT

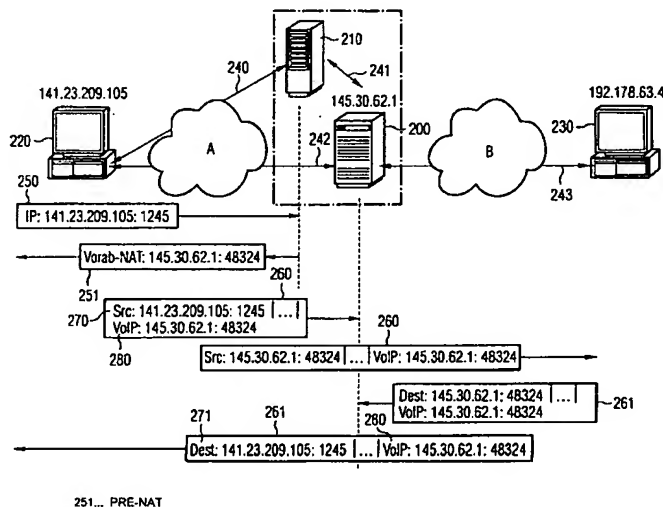
(10) Internationale Veröffentlichungsnummer
WO 03/028340 A1

- (51) Internationale Patentklassifikation⁷: **H04L 29/12**, 29/06 (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).
- (21) Internationales Aktenzeichen: **PCT/DE02/02840** (72) Erfinder; und
- (22) Internationales Anmeldedatum: **1. August 2002 (01.08.2002)** (75) Erfinder/Anmelder (nur für US): **KLAGHOFER, Karl** [AT/DE]; Krüner Strasse 12, 81373 München (DE). **MÜLLER, Harald** [DE/DE]; Flurgrenzstr. 36, 82205 Gilching (DE). **TOTZKE, Jürgen** [DE/DE]; Blumenstr. 49, 85586 Poing (DE). **VOLKMANN, Gerald** [DE/DE]; Himalajastr. 32, 81825 München (DE).
- (25) Einreichungssprache: **Deutsch**
- (26) Veröffentlichungssprache: **Deutsch**
- (30) Angaben zur Priorität: **101 42 500.7** **30. August 2001 (30.08.2001)** **DE** (74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: PRE- PROCESSING OF NAT ADDRESSES

(54) Bezeichnung: VORABAUSHANDLUNG VON NAT-ADRESSEN



WO 03/028340 A1

(57) Abstract: A method for packet-oriented transmission of speech, audio, video and/or useful data between an internal (A) and a public data network (B) by means of a pre-reservation of NAT addresses. A pre-NAT address (251) is allocated to the IP address (250) of an internal computer (220) by an NAT address server (210). The relevant allocation data set is available in a NAT host 200 which acts as a gateway between the internal (A) and the public data network (B); whereby single addresses (pre- NAT addresses) are provided for transparent use of the data packet in the internal and public network when the information on the origin (270) or destination (271) in an IP Header (260, 261) or in the protocol data, in addition to the information on origin or destination in said header, is modified.

(57) Zusammenfassung: Verfahren zur paketorientierten Übermittlung von Sprach-, Audio-, Video- und/oder Nutzdaten zwischen einem internen (A) und einem öffentlichen Datennetz (B) durch eine Vorab-Reservierung von NAT-Adressen. Eine Vorab-NAT-Adresse (251) zur IP-Adresse (250) eines internen Rechners (220) wird durch einen NAT-Adressserver (210)

[Fortsetzung auf der nächsten Seite]



(81) Bestimmungsstaaten (*national*): CN, US.

— Erfindererklärung (Regel 4.17 Ziffer iv) nur für US

(84) Bestimmungsstaaten (*regional*): europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

Veröffentlicht:

- mit internationalem Recherchenbericht
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

Erklärungen gemäß Regel 4.17:

- hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten CN, europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR)

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

zugeordnet. Der aktuelle Zuordnungsdatensatz liegt an einem NAT-Host 200, welcher als Schnittstellenrechner (Gateway) zwischen dem internen (A) und dem öffentlichen Datennetz (B) fungiert, vor, wodurch beim Abändern von Herkunfts- (270) bzw. Zielangaben (271) im Kopf eines Datenpakets (IP-Header) (260, 261) sowohl in den Protokolldaten wie auch in der Herkunfts- bzw. Zielangabe im Kopf desselben einheitliche Adressen (Vorab-NAT-Adressen) für eine transparente Nutzung des Datenpakets im internen wie im öffentlichen Datennetz vorliegen.

Beschreibung

Vorabaushandlung von NAT-Adressen

- 5 Die Erfindung betrifft ein Verfahren nach dem Oberbegriff des Anspruchs 1 sowie eine Anordnung zur Durchführung des Verfahrens nach dem Oberbegriff des Anspruchs 4.

Verfahren der in Rede stehenden Art werden heute in breitem
10 Umfang zur Übermittlung von Sprach-, Audio-, Video- und/oder Nutzdaten über Netzwerkgrenzen, z. B. zwischen internen und öffentlichen Datennetzen, hinweg eingesetzt. Bei der Übermittlung von Daten über IP-Netze treten immer wieder Probleme auf, wenn an einer Netzwerkgrenze eine
15 Adreßumsetzung mit NAT (Network Address Translation) erfolgt. NAT ist dabei aus verschiedenen Gründen von wesentlicher Bedeutung für die Internettechnologie. Neben der Bereitstellung einer Lastverteilung im Parallel-Processing werden verschiedene Arten von Zugangssicherungen im Sinne
20 eines Firewalls sowie Fehlertoleranz und Hochverfügbarkeit unterstützt. Weiterhin werden grundlegende Funktionen der Netzwerkadministration vereinfacht.

Da der in den Gründungsjahren des Internet vorgesehene
25 Adreßraum für die Vergabe von IP-Adressen auf absehbare Zeit nicht mehr ausreichen wird, insbesondere der Ausbau von internen und hochkomplexen Datennetzen mehr und mehr IP-Adressen erfordert, wird NAT aber vor allem eingesetzt, um die intern benutzten IP-Adressen nach außen zu verbergen.
30 Dies macht zum einen die Verwaltung interner Netze einfacher, zum anderen werden Kosten gespart, da man nach außen weniger öffentliche kostenpflichtige IP-Adressen benutzen muß als man intern wirklich gebraucht. Im Prinzip ist es dabei theoretisch möglich, ein internes lokales Netz von bis zu
35 60000 Rechnern auf eine einzige öffentliche IP-Adresse abzubilden, indem man die Portadresse der öffentlichen IP-Adresse variiert.

Bei NAT wird zunächst beim Versenden eines IP-Datenpakets der IP-Header dieses Pakets ausgetauscht. Die interne IP-Adresse inklusive Portnummer wird durch eine öffentliche IP-Adresse mit einer anderen Portnummer ersetzt. Ein NAT-Host speichert die Zuordnung (Mapping) von interner IP-Adresse auf die öffentliche (externe) IP-Adresse. Empfängt nun der NAT-Host ein IP-Datenpaket, so bildet er die öffentliche (externe) IP-Adresse wieder auf die interne IP-Adresse ab. Der NAT-Host ist dabei als ein zwei Netzwerke miteinander verbindender Rechner zu verstehen, auf welchem eine entsprechende Software (NAT-Engine) für die Adreßumsetzung sorgt.

Problematisch ist allerdings, daß einige IP-Protokolle die internen IP-Adressen als Protokolldaten noch einmal mitschicken (z. B. bei Voice-over-IP-Protokollen). Am NAT-Host werden nur die IP-Header eines Datenpakets ausgetauscht, nicht aber auf die Protokolldaten selbst zugegriffen, da diese vom NAT-Host nicht auflösbar sind. Der adressierte externe Rechner im öffentlichen Netz schickt nun seine Antwort nicht zu der öffentlichen Adresse im IP-Header des Datenpakets, sondern zu der internen IP-Adresse, die der verwendete Dienst (z. B. Voice-over-IP) aus den Protokolldaten herausgelesen hat. Unter dieser Adresse ist der ursprüngliche Sender jedoch nicht erreichbar. Damit geht die Antwort entweder einer unbekannten IP-Adresse oder einem anderen öffentlichen Rechner zu, der mit diesem IP-Datenpaket nichts anfangen kann.

Das hier geschilderte Problem wurde bislang noch nicht gelöst. Zwar gibt es vereinzelte Ansätze, direkt auf dem NAT-Host einen Protokoll-Analyzer einzusetzen, welcher in der Lage ist, bestimmte Protokolle auszupacken und hier neben dem IP-Header auch die Protokolldaten entsprechend der NAT-Zuordnung (Mapping) zu verändern. Dieser regelmäßige Zugriff auf Protokolldaten sowie deren Analyse würden allerdings den Datenverkehr nicht unerheblich verlangsamen. Außerdem müßten

je nach eingesetztem Protokolltyp möglicherweise nicht nur ein, sondern mehrere Protokoll-Analyzer eingesetzt werden. Künftig könnte durch IPv6 (Internet Protocol Version 6 - mit erweitertem IP-Adreßraum) das Problem gelöst werden, aber
5 IPv6 wird noch lange nicht durchgängig implementiert sein. Durch das erheblich gestiegene Interesse der Firmen an Internet-Telefonie und den Austausch von Bild- und Nutzdaten ist allerdings eine rasche und sichere Lösung der geschilderten Problematik von Nöten.

10

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren bereitzustellen, welches unter Beibehaltung bestehender NAT-Konfigurationen den Aufbau transparenter Verbindungen für komplexere Protokolle (Sprach-, Audio-, Video- und/oder
15 Nutzdaten) über einen NAT-Host ermöglicht.

Es ist weiterhin Aufgabe der vorliegenden Erfindung, eine Anordnung zur Durchführung des erfindungsgemäßen Verfahrens bereitzustellen.

20

Ein Kerngedanke des erfindungsgemäßen Verfahrens besteht darin, auf der einen Seite die Nutzung von komplexeren Protokollen (z. B. Voice-over-IP) in unverändertem Umfang so zu unterstützen, daß die Probleme bei der Adressierung von
25 Rechnern im öffentlichen IP-Netz, welche allein durch den Einsatz von NAT entstehen, gelöst werden. Dies wird bei der paketorientierten Übermittlung von Sprach-, Audio-, Video- und/oder Nutzdaten zwischen einem internen und einem öffentlichen Datennetz durch eine Vorab-Reservierung von NAT-
30 Adressen ermöglicht, wobei zunächst eine Anfrage eines internen Rechners an einen NAT-Adreßserver zum Bereitstellen einer Vorab-NAT-Adresse zu einer IP-Adresse des internen Rechners gesandt wird. Diese Vorab-NAT-Adresse zur IP-Adresse des internen Rechners wird durch den NAT-Adreßserver
35 zugeordnet. Der aktuelle Zuordnungsdatensatz zwischen der Vorab-NAT-Adresse und der IP-Adresse des internen Rechners wird vom NAT-Adreßserver schließlich an einen NAT-Host

gesandt. Damit liegt am NAT-Host, welcher als Schnittstellenrechner (Gateway) zwischen dem internen und dem öffentlichen Datennetz fungiert, der aktuelle Zuordnungsdatensatz zum Abändern von Herkunfts- bzw.

5 Zielangaben im Kopf eines Datenpaketes (IP-Header) vor. Im nächsten Schritt wird die Vorab-NAT-Adresse des internen Rechners von dem NAT-Adreßserver an den internen Rechner gesandt. Am Rechner wird diese Vorab-NAT-Adresse von der entsprechenden Dienst (z. B. Voice-over-IP) als

10 Absenderadresse in die Protokolldaten eines Datenpakets eingebracht. Von dem internen Rechner wird nun ein Datenpaket, insbesondere mit Voice-over-IP-Protokolldaten, welche als Voice-over-IP-Adresse nunmehr die Vorab-NAT-Adresse enthalten, an den NAT-Host gesandt. Auf diesem kann

15 im nächsten Schritt eine Herkunftsangabe im Kopf des Datenpakets (IP-Header), welche die IP-Adresse des internen Rechners enthält, gegen die zugeordnete Vorab-NAT-Adresse ausgetauscht werden. Damit liegen sowohl in den Protokolldaten des Datenpakets wie auch in der

20 Herkunftsangabe im Kopf desselben einheitliche Adressen (Vorab-NAT-Adressen) für eine transparente Nutzung des Datenpakets im internen wie im öffentlichen Datennetz vor. Das Datenpaket wird schließlich durch den NAT-Host an einen extern adressierten Rechner weitergeleitet.

25

Der Vorteil dieser Lösung besteht darin, daß sich der NAT-Host um die Protokolldaten nicht mehr kümmern muß. Der oder die internen Rechner (Clients) können den NAT-Server kontaktieren, um ihre zukünftige NAT-Adresse schon im Vorfeld

30 zu erfahren. Diese wird beim Zusammenstellen der Protokolldaten berücksichtigt. Der externe Rechner im öffentlichen Datennetz erhält nun in den Protokolldaten die korrekte Antwortadresse, welche dann dem NAT-Host zugeht und dieser die Rückantwort korrekt dem internen Rechner zustellen

35 kann. Der NAT-Host wird zudem entlastet, da er nun nicht selbst das Datenpaket entsprechend dem verwendeten Protokoll auspacken muß, sondern wie herkömmlich nur die

Herkunftsangabe im Kopf des Datenpakets (IP-Header) austauscht.

Vorteilhafte Weiterbildungen des erfindungsgemäßen Verfahrens
5 sind in den Unteransprüchen 2 und 3 angegeben.

Bevorzugt wird das Datenpaket mit der Vorab-NAT-Adresse von dem extern adressierten Rechner durch den NAT-Host empfangen. Dieser kann im nächsten Schritt durch Austauschen einer
10 Zielangabe im Kopf des Datenpakets (IP-Header), welche der Vorab-NAT-Adresse entspricht, gegen die zugeordnete IP-Adresse des internen Rechners unter Verwendung des aktuellen Zuordnungsdatensatzes austauschen. Im nächsten Schritt wird dann das Datenpaket durch den NAT-Host an den intern
15 adressierten Rechner weitergeleitet. Ein besonderer Vorteil entsteht dadurch, daß das üblicherweise durchgeführte Austauschen der Zielangabe im Kopf des Datenpakets (IP-Header) von dem extern adressierten Rechner im üblichen Rahmen unverändert beibehalten werden kann. Dadurch, daß nun
20 aber transparente Adressen in der Zielangabe im Kopf des Datenpakets (IP-Header) und in den mit diesem Datenpaket transportierten Protokolldaten vorliegen, ist eine Fehlleitung des Datenpakets ausgeschlossen.

25 Bevorzugt erfragt der NAT-Host den aktuellen Zuordnungsdatensatz beim NAT-Adreßserver, bevor der eigentliche Austausch der Zielangabe im Kopf des Datenpakets (IP-Header) des externen Rechners durchgeführt wird. Dadurch wird eine Doppeltvergabe von Vorab-NAT-Adressen an
30 Datenpakete, welche nicht das Resultat einer Anfrage aus dem internen in das öffentliche Netz hinein sind, vermieden. Der Austausch der Zielangabe im Kopf eines vom öffentlichen in das interne Netz geschickten Datenpakets (IP-Header) kann dann unter Berücksichtigung des aktuellen
35 Zuordnungsdatensatzes schon vergebener IP-Adressen durchgeführt werden.

Die Aufgabe der vorliegenden Erfindung wird weiterhin durch eine Anordnung zum Durchführen des erfindungsgemäßen Verfahrens gelöst.

- 5 Dabei wird, zusätzlich zu einem NAT-Host, welcher wenigstens ein internes Datennetz mit einem öffentlichen Datennetz verbindet und wenigstens einem internen Rechner, welcher über den NAT-Host mit einem öffentlichen Rechner kommuniziert oder kommunizieren kann, ein NAT-Adreßserver bereitgestellt,
- 10 welcher mit dem internen Rechner und dem NAT-Host in Verbindung steht oder in Verbindung treten kann, und welcher zum Ermitteln und Zuordnen von Vorab-NAT-Adressen zur IP-Adresse eines internen Rechners dient.
- 15 Das Ermitteln von Vorab-NAT-Adressen schließt dabei die Verwaltung (Hinzufügung, Aktualisierung, Löschung) der schon vergebenen Zuordnungen mit ein, um eine Doppeltvergabe von Vorab-NAT-Adressen zu IP-Adressen von internen Rechnern zu vermeiden. Unter einer Adresse (Vorab-NAT-Adresse, IP-
- 20 Adresse) wird hier grundsätzlich die IP-Nummer (z. B. 141.23.209.105) zusammen mit einer Portnummer (z. B. 1245) verstanden. Da die IP-Nummer des NAT-Hosts immer gleich ist, wird die Zuordnung der Vorab-NAT-Adresse über die Vergabe einer Portnummer zur IP-Nummer des NAT-Hosts gelöst, welche
- 25 schließlich die IP-Adresse (IP-Nummer und Portnummer) des internen Rechners referenziert.

Vorteilhafte Weiterbildungen der erfindungsgemäßen Anordnung sind in den Unteransprüchen 5 und 6 angegeben.

- 30 Bevorzugt läuft dabei der NAT-Adreßserver zusammen mit dem NAT-Host auf einem gemeinsamen Rechner ab. Der NAT-Host kann dabei Funktionalitäten eines Gatekeepers wie Adreßumsetzung, Zugangskontrolle, Bandbreitenkontrolle, usw. von
- 35 Multimediadiensten wahrnehmen. Durch die enge Kopplung des NAT-Hosts und seinen speziellen Diensten mit dem NAT-Adreßserver auf einem gemeinsamen Rechner werden insbesondere

Kommunikationsprotokolle über das Datennetz vermieden. Der NAT-Adreßserver kann dem entsprechend schnell benutzter bzw. freie IP_-Adressen vom NAT-Host erfragen, bevor eine Zuordnung zu IP-Adressen interner Rechner vorgenommen wird.

5

Von besonderem Vorteil ist auch, wenn standardisierte Protokolle, insbesondere SIP (Session Initiation Protocol) oder H.323, zur Übermittlung von Sprach-, Audio- und/oder Videodatenpaketen über Netzwerkverbindungen genutzt werden.

10 Diese Protokolle bieten im Zusammenhang mit der erfindungsgemäßen Anordnung Mechanismen für Rufweiterleitung, Rufsignalsisierung, Aufnahme unterstützender Daten, Medienkontrolle und ergänzender Dienste. Dabei ist H.323 ein bewährtes Protokoll, welches insbesondere wegen seiner

15 Benutzungsfreundlichkeit, Verlässlichkeit und Interoperabilität mit PSTN (Public Switched Telephone Network) genutzt wird. SIP ist ein neues Protokoll, welches Skalierbarkeit, Flexibilität und leichte Implementierbarkeit beim Aufbau komplexer Systeme garantiert.

20

Die Erfindung wird im folgenden anhand eines Ausführungsbeispiels näher erläutert. Es zeigen:

Fig. 1 eine erfindungsgemäße Anordnung zur paketorientierten

25 Übermittlung von Sprach-, Audio-, Video- und/oder Nutzdaten zwischen einem internen A und einem öffentlichen Datennetz B gemäß dem Stand der Technik und

Fig. 2 eine erfindungsgemäße Anordnung zur paketorientierten

30 Übermittlung von Sprach-, Audio-, Video- und/oder Nutzdaten zwischen einem internen A und einem öffentlichen Datennetz B.

Zur Verdeutlichung der von der Erfindung gelösten Problematik wird in Fig. 1 in einer Anordnung gemäß dem Stand der Technik

35 die Problematik noch einmal erläutert. Dabei verbindet ein NAT-Host 100 mit der IP-Nummer 145.30.62.1 ein internes A mit einem öffentlichen Datennetz B. Ein Rechner 120 mit der IP-

Nummer 141.23.209.105 steht über den NAT-Host 100 mit einem weiteren Rechner 130 mit der IP-Nummer 192.178.63.4 in Verbindung. Beim Aufbau einer Kommunikation zwischen den Rechnern 120, 130 wird zunächst ein Datenpaket 160 über eine Netzwerkverbindung 142 von dem internen Rechner 120 an den NAT-Host 100 gesandt. Als Herkunftsangabe 170 des Datenpaketes wird die IP-Adresse (bestehend aus IP-Nummer und Portnummer) des Rechners 120, nämlich 141.23.209.105:1245 verwandt. In den Protokolldaten findet sich die von dem auf dem Rechner 120 laufenden spezifischen Dienst verwendete Voice-over-IP-Adresse 180, welche identisch mit der IP-Adresse des Rechners 120 ist, wieder.

Auf dem NAT-Host 100 wird nun die Herkunftsangabe des Datenpakets 160, also die IP-Adresse 141.23.209.105:1245 des Rechners 120 durch die öffentlich sichtbare IP-Nummer 145.30.62.1 des NAT-Host 100 zusammen mit einer zugeordneten Portnummer, nämlich 48324 ersetzt. Über diese Portnummer 48324 kann eine Zuordnung (Mapping) der geänderten Herkunftsangabe zur ursprünglichen Herkunftsangabe, also der IP-Adresse 141.23.209.105:1245 des Rechners 120 vorgenommen werden. Bei dieser Änderung der Herkunftsangabe des Datenpakets 160 bleibt allerdings die Voice-over-IP-Adresse 180 weiterhin 141.23.209.105:1245 und damit gleich der ursprünglichen IP-Adresse des Rechners 120.

Dieses Datenpaket 160 wird über die Netzwerkverbindung 143 an den Rechner 130 weitergeleitet. Dieser Rechner 130 wiederum empfängt die Nachricht und verwendet für den Verbindungsaufbau die von dem entsprechenden Dienst, hier Voice-over-IP, in den Protokolldaten des Datenpakets 160 vorliegende Voice-over-IP-Adresse. Damit aber wird das zurückgeschickte Datenpaket 161 des Rechners 130 an die ursprüngliche IP-Adresse des Rechners 120 adressiert. Mit der Zielangabe 171 des Datenpakets 161, also der IP-Adresse 141.23.209.105:1245, geht die Antwort damit entweder zu einer unbekannten IP-Adresse oder zu einem anderen öffentlichen

Rechner, der mit diesem Datenpaket nichts anfangen kann. Die geschilderte Problematik besteht also darin, daß am NAT-Host 100 eine Adreßumsetzung stattfindet, welche zwar die Herkunfts- 170 bzw. Zielangabe 171 (den IP-Header) des Datenpakets 160 bzw. 161 verändert, die relevante Voice-over-IP-Adresse 180 für den verwendeten Voice-over-IP-Dienst aber unberührt läßt. Gerade dieser Dienst adressiert aber in der Zielangabe 171 des rückkehrenden Datenpaketes 161 die IP-Adresse, welche für den Dienst in den für ihn bestimmten Protokolldaten hinterlegt war.

In Fig. 2 ist nun eine erfindungsgemäße Anordnung dargestellt, bei der wiederum ein NAT-Host 200 ein internes A mit einem öffentlichen Datennetz B verbindet. Der NAT-Host 200 mit der IP-Nummer 145.30.62.1 kommuniziert bidirektional mit einem NAT-Adreßserver 210, wobei NAT-Host 200 und NAT-Adreßserver 210 mit einem internen Rechner 220 mit der IP-Nummer 141.23.209.105 über Netzwerkverbindungen 240 bzw. 242 in Verbindung stehen. NAT-Host und NAT-Adreßserver können auch auf einem gemeinsamen Rechner laufen, sind hier aber zur Verdeutlichung des Funktionsprinzips der erfindungsgemäßen Anordnung getrennt dargestellt. Der Rechner 220 steht über den NAT-Host 200 mit einem weiteren Rechner 230 mit der IP-Nummer 192.178.63.4 in Verbindung.

Um die vorab geschilderte Problematik auszuschließen, sendet der Rechner 220 über die Netzwerkverbindung 240 zunächst eine Anfrage an den NAT-Adreßserver 210, ihm zu seiner IP-Adresse 250, in diesem Fall 141.23.209.105:1245, eine Vorab-NAT-Adresse 251 zuzuordnen. Der NAT-Adreßserver 210 bestimmt zunächst eine noch nicht zugeordnete Vorab-NAT-Adresse 251, welche er schließlich über die Netzwerkverbindung 240 dem Rechner 220 zukommen läßt. Die Vorab-NAT-Adresse im vorliegenden Ausführungsbeispiel lautet 145.30.62.1:48324. Über die Portnummer 48324 der Vorab-NAT-Adresse läßt sich somit eine Zuordnung (Mapping) zu der IP-Adresse 141.23.209.105:1245 des Rechners 220 vornehmen. Die IP-Nummer

145.30.62.1 der Vorab-NAT-Adresse 251 entspricht der IP-Nummer des NAT-Hosts 200, welche nach außen in das öffentliche Netz B sichtbar ist.

- 5 Im nächsten Schritt sendet der Rechner 220 schließlich ein Datenpaket 260 an den NAT-Host 200, in dessen Protokolldaten sich die zugeteilte Vorab-NAT-Adresse 145.30.62.1:48324 als Voice-over-IP-Adresse 280 wiederfindet. Die Herkunftsangabe 270 im Kopf des Datenpakets (IP-Header) 260 lautet dagegen
- 10 auf die IP-Adresse des Rechners 220, nämlich 141.23.209.105:1245. Auf dem NAT-Host 200 wird wiederum eine Adreßumsetzung der Herkunftsangabe 270 des Datenpakets vorgenommen, bei der die IP-Adresse des Rechners 220 gegen die vom NAT-Adreßserver 210 zugeteilte Vorab-NAT-Adresse
- 15 145.30.62.1:48324. Diese aktuelle Zuordnung der Vorab-NAT-Adresse zu der IP-Adresse des Rechners 220 (Mapping) wird dem NAT-Host 200 nach der Vergabe der Vorab-NAT-Adresse durch den NAT-Adreßserver 210 über die Netzwerkverbindung 241 mitgeteilt oder vom NAT-Host 200 erfragt. Die IP-Adresse des
- 20 internen Rechners 220 kann nunmehr über die Zuordnung der Portnummer 48324 zu der IP-Adresse des internen Rechners 220, nämlich 141.23.209.105:1245 zurückverfolgt werden.

- In einem weiteren Schritt wird von dem NAT-Host 200 das
- 25 Datenpaket 260 an den externen Rechner 230 über die Netzwerkverbindung 243 gesandt. Der dort verwendete Dienst Voice-over-IP nutzt die in den Protokolldaten zu findende Voice-over-IP-Adresse 280, welche nunmehr der Vorab-NAT-Adresse 251 entspricht, als Zielangabe 271 zur Rücksendung des Datenpakets 261. Diese Zielangabe 271 lautet nun auf
- 30 145.30.62.1:48324.

- Diese adressiert den NAT-Host 200, wo auf Basis der aktuellen Zuordnung die Zielangabe 271 im Kopf des Datenpakets (IP-
- 35 Header) 261 gegen die tatsächliche IP-Adresse des im Rechners 220, also die Vorab-NAT-Adresse 145.30.62.1:48324 gegen die IP-Adresse 141.23.209.105:1245 ausgetauscht wird. Damit kann

das Datenpaket 261 vom NAT-Host 200 dem Rechner 220 zugeordnet und an diesen versandt werden.

5 In den Protokolldaten wird für den Voice-over-IP-Verbindungs-
aufbau insbesondere das Protokoll H.323 oder SIP verwendet.
Damit ist mit der erfindungsgemäßen Anordnung zur
Durchführung des Verfahrens grundsätzlich auch die
Kommunikation zwischen einem oder mehreren internen Rechnern
(Multipoint-Connection) und einem oder mehreren externen
10 Rechnern auf Basis von Sprach-, Audio-, Video- und/oder
Nutzdaten gewährleistet.

An dieser Stelle sei darauf hingewiesen, daß alle oben
beschriebenen Teile für sich alleine gesehen und in jeder
15 Kombination, insbesondere die in den Zeichnungen
dargestellten Details als erfindungswesentlich beansprucht
werden. Abänderungen hiervon sind dem Fachmann geläufig.

Patentansprüche

1. Verfahren zur paketorientierten Übermittlung von Sprach-, Audio-, Video- und/oder Nutzdaten zwischen einem internen und
5 einem öffentlichen Datennetz, mit folgenden Verfahrensschritten:
- a) Senden einer Anfrage eines internen Multimedia-Rechners (220) an einen NAT-Adress-Server (210) (NAT: Network Address Translation) zum Bereitstellen einer Vorab-NAT-Adresse (251)
10 zu einer IP-Adresse (250) (IP: Internet Protocol) des internen Rechners;
- b) Zuordnen einer Vorab-NAT-Adresse (251) zur IP-Adresse des internen Rechners durch den NAT-Adress-Server;
- c) Senden eines aktuellen Zuordnungs-Datensatzes zwischen der
15 Vorab-NAT-Adresse und der IP-Adresse des internen Rechners vom NAT-Adress-Server an einen NAT-Host (200);
- d) Senden der Vorab-NAT-Adresse des internen Rechners von dem NAT-Adress-Server an den internen Rechner;
- e) Senden eines Datenpakets (260) mit Protokolldaten, welche
20 die Vorab-NAT-Adresse enthalten, vom internen Rechner an den NAT-Host;
- f) Austauschen einer Herkunftsangabe (270) im Kopf des Datenpakets (260), welche die IP-Adresse des internen Rechners enthält, gegen die zugeordnete Vorab-NAT-Adresse;
- 25 g) Weiterleiten des Datenpakets durch den NAT-Host an einen extern adressierten Rechner (230).
2. Verfahren nach Anspruch 1, mit folgenden weiteren Verfahrensschritten:
- 30 h) Empfangen eines Datenpakets (261) mit der Vorab-NAT-Adresse von dem extern adressierten Rechnern durch den NAT-Host;
- i) Austauschen einer Zielangabe (271) im Kopf des Datenpakets (IP-Header) (261), welche die Vorab-NAT-Adresse enthält,
35 gegen die zugeordnete IP-Adresse des internen Rechners unter Verwendung des aktuellen Zuordnungs-Datensatzes durch den NAT-Host;

j) Weiterleiten des Datenpakets durch den NAT-Host an den intern adressierten Rechner.

3. Verfahren nach Anspruch 1, bei dem vor dem

- 5 Verfahrensschritt i) der weitere Schritt des Abfragens des aktuellen Zuordnungs-Datensatzes vom NAT-Host (200) gegen den NAT-Adress-Server (210) durchgeführt wird.

- 10 4. Anordnung zum Durchführen des Verfahrens nach einem der vorstehenden Ansprüche, mit
- einem NAT-Host (200), welcher wenigstens ein internes Datennetz mit einem öffentlichen Datennetz verbindet, zum Austauschen der Ziel- (271) und/oder Herkunfts-IP-Adressen (270) ein- und/oder ausgehender Datenpakete (260,261); und
 - 15 - wenigstens einem internen Rechner (220), welcher über den NAT-Host mit wenigstens einem öffentlichen Rechner (230) in Verbindung steht oder in Verbindung treten kann,
- g e k e n n z e i c h n e t d u r c h
- einen NAT-Adress-Server (210), welcher mit dem internen
 - 20 Rechner und dem NAT-Host in Verbindung steht oder in Verbindung treten kann, zum Ermitteln und Zuordnen von Vorab-NAT-Adressen (251) zur IP-Adresse (250) eines internen Rechners.

- 25 5. Anordnung zum Durchführen des Verfahrens nach einem der Ansprüche 3 oder 4,
- d a d u r c h g e k e n n z e i c h n e t, daß
- der NAT-Adress-Server (210) zusammen mit dem NAT-Host (200) auf einem gemeinsamen Rechner abläuft.

30

6. Anordnung zum Durchführen des Verfahrens nach einem der vorhergehenden Ansprüche,
- g e k e n n z e i c h n e t d u r c h
- standardisierte Protokolle, insbesondere SIP oder H.323, zur
- 35 Übermittlung von Sprach-, Audio- und/oder Video-Datenpaketen über Netzwerkverbindungen (240,241,242,243).

FIG 1

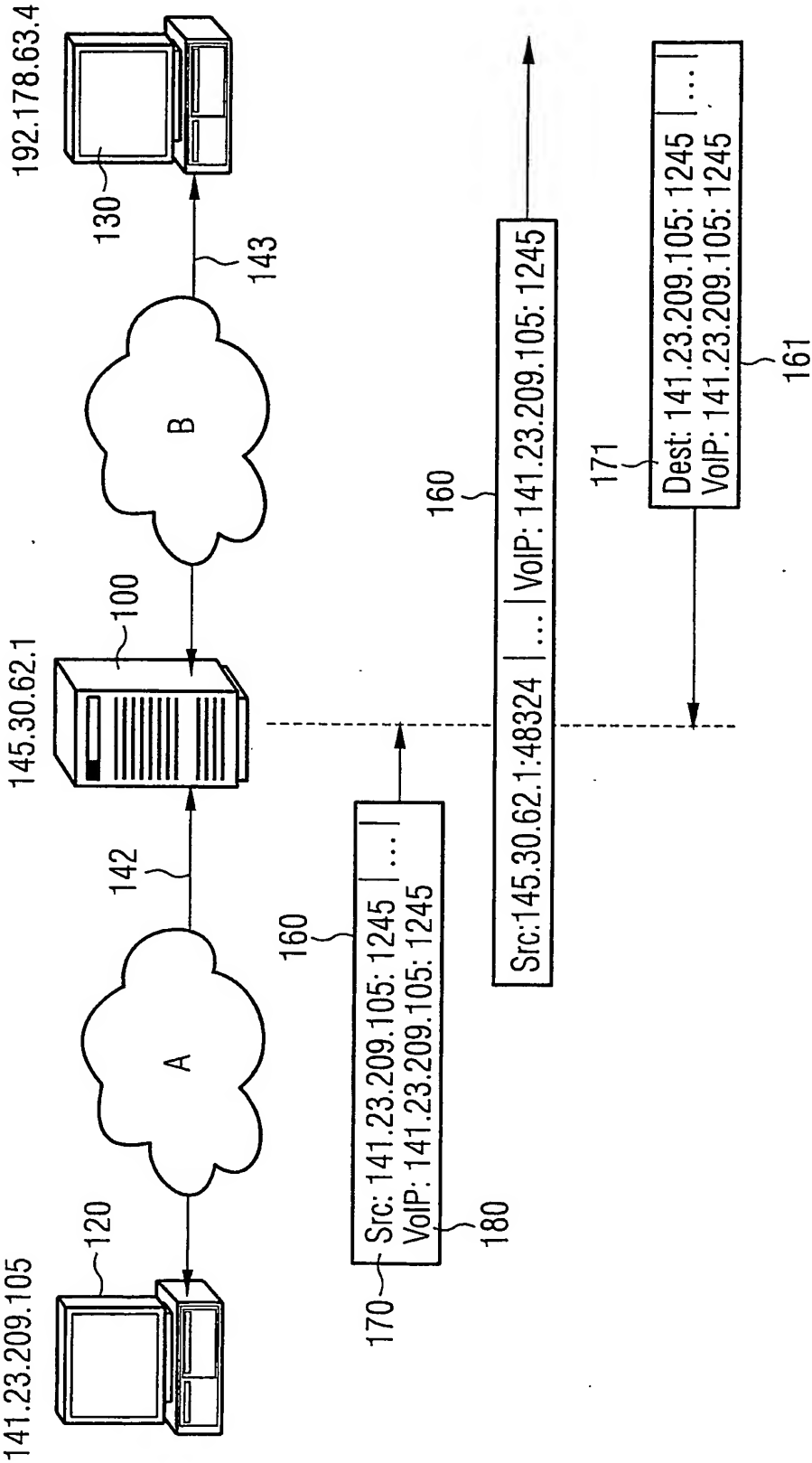
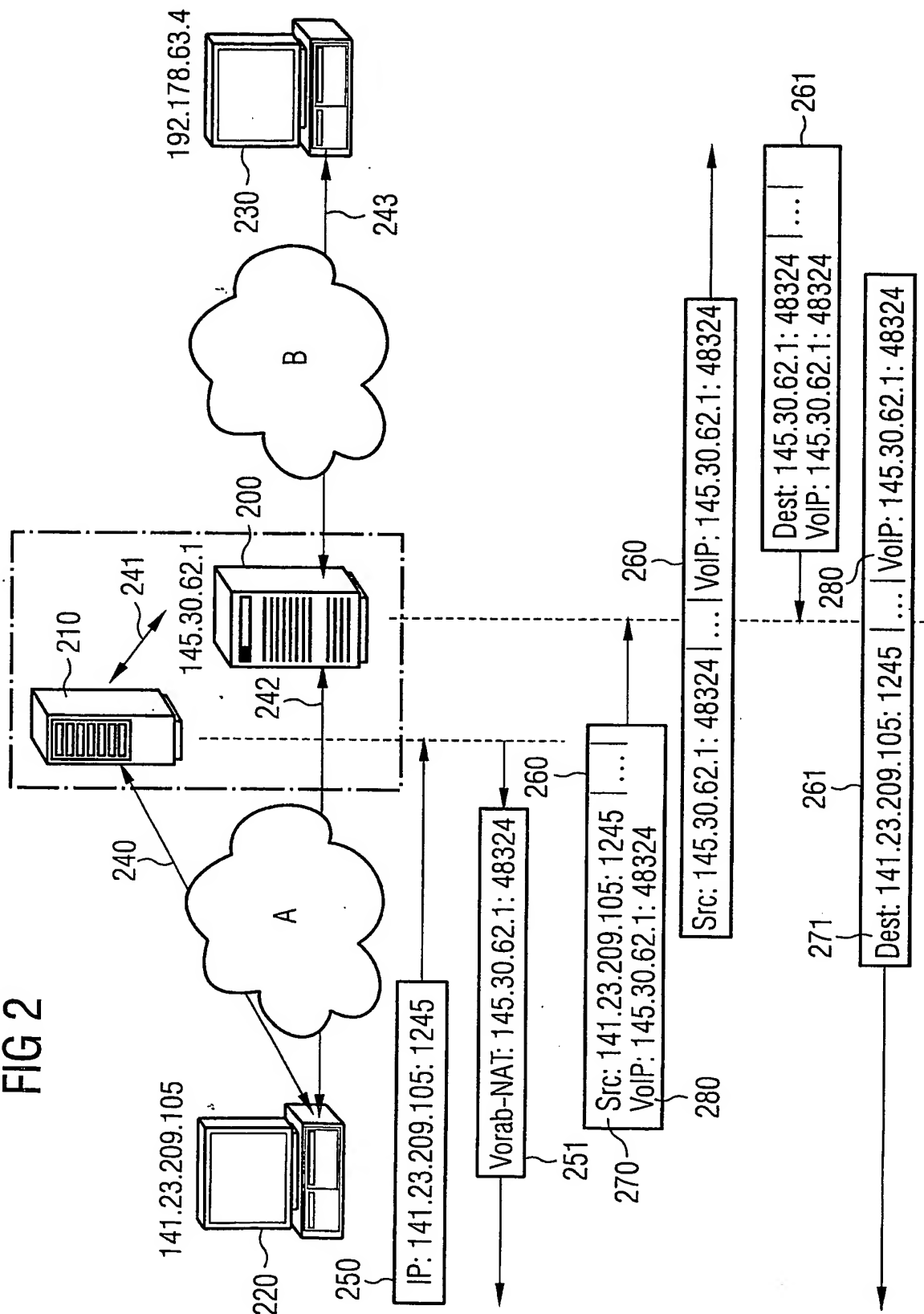


FIG 2



INTERNATIONAL SEARCH REPORT

National Application No.

PCT/DE 02/02840

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L29/12 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BRUSTOLONI J C; GARAY J A: "Application-independent End-to-End Security in Shared-Link Access Networks" PROCEEDINGS OF THE NETWORKING 2000 CONFERENCE; IFIP, PARIS, FRANCE; LECTURE NOTES IN COMPUTER SCIENCE, vol. 1815, May 2000 (2000-05), pages 608-619, XP001148130 abstract Abschnitte 1., 4., 6. --- -/-	1, 2, 4-6



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- *&* document member of the same patent family

Date of the actual completion of the international search

29 January 2003

Date of mailing of the international search report

06/02/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Kesting, V

INTERNATIONAL SEARCH REPORT

International Application No

PCT/DE 02/02840

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	WO 02 23822 A (ARAVOX TECHNOLOGIES ;MOLITOR ANDREW T (US)) 21 March 2002 (2002-03-21) page 2, line 13 -page 5, line 19 page 6, line 25 - line 26 page 10, line 1 - line 19 page 12, line 10 -page 14, line 6 page 15, line 3 - line 12 page 15, line 19 -page 16, line 14 page 21, line 5 - line 9 -----	1,2,4-6
A	THERNELIUS F: "SIP, NAT, and Firewalls" MASTER THESIS, May 2000 (2000-05), pages 1-69, XP002209773 Kapitel 11 -----	1,2,4-6

INTERNATIONAL SEARCH REPORT

Information on patent family members

al Application No

PCT/DE 02/02840

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
WO 0223822	A	21-03-2002	AU	8705401 A	26-03-2002
			WO	0223822 A1	21-03-2002

INTERNATIONALER RECHERCHENBERICHT

des Aktenzeichens

PCT/DE 02/02840

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 IPK 7 H04L29/12 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, INSPEC, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	BRUSTOLONI J C; GARAY J A: "Application-independent End-to-End Security in Shared-Link Access Networks" PROCEEDINGS OF THE NETWORKING 2000 CONFERENCE, IFIP, PARIS, FRANCE; LECTURE NOTES IN COMPUTER SCIENCE, Bd. 1815, Mai 2000 (2000-05), Seiten 608-619, XP001148130 Zusammenfassung Abschnitte 1., 4., 6. --/--	1,2,4-6



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

29. Januar 2003

Absendedatum des internationalen Recherchenberichts

06/02/2003

Name und Postanschrift der internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Kesting, V

INTERNATIONALER RECHERCHENBERICHT

nales Aktenzeichen

PCI/DE 02/02840

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P, X	WO 02 23822 A (ARAVOX TECHNOLOGIES ;MOLITOR ANDREW T (US)) 21. März 2002 (2002-03-21) Seite 2, Zeile 13 -Seite 5, Zeile 19 Seite 6, Zeile 25 - Zeile 26 Seite 10, Zeile 1 - Zeile 19 Seite 12, Zeile 10 -Seite 14, Zeile 6 Seite 15, Zeile 3 - Zeile 12 Seite 15, Zeile 19 -Seite 16, Zeile 14 Seite 21, Zeile 5 - Zeile 9 -----	1,2,4-6
A	THERNELIUS F: "SIP, NAT, and Firewalls" MASTER THESIS, Mai 2000 (2000-05), Seiten 1-69, XP002209773 Kapitel 11 -----	1,2,4-6

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

is Aktenzeichen

PCT/DE 02/02840

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 0223822	A	21-03-2002	AU	8705401 A	26-03-2002
			WO	0223822 A1	21-03-2002

THIS PAGE BLANK (USPTO)